

Canal TI

La revista del negocio TI del Perú

Nº 941

LUNES 5
MAYO
2025

AGI

ESET Latinoamérica

advierte que los modelos de IA son objetivos
valiosos para los cibercriminales

Las ventajas de las impresoras multifuncionales de inyección de tinta



Daniel Hoyos, Product Manager de EcoTank y Consumibles en Epson Latinoamérica.

Epson

Ahorro y conectividad para imprimir en casa

Con el inicio del nuevo ciclo académico, contar con una impresora eficiente se ha convertido en una necesidad para estudiantes y familias. Desde la impresión de tareas y trabajos de investigación hasta material didáctico y documentos administrativos, elegir la herramienta de impresión adecuada puede transformar la rutina de estudio y mejorar el rendimiento académico.

Las impresoras multifuncionales de inyección a tinta permiten impresión de bajo costo y con mayor ahorro energético que sus contrapartes láser, permitiendo hasta 6,000 a color y 7,500 en blanco y negro con un solo kit de tinta. Además, debido a que pueden escanear y fotocopiar, contribuyen a la organización del hogar. Para elegir la impresora ideal, los especialistas de Epson sugieren considerar tres aspectos clave que asegurarán una inversión inteligente y un rendimiento óptimo.

Calidad de impresión y eficiencia

La nitidez y fidelidad de los colores son esenciales para obtener documentos legibles y gráficos bien definidos. Optar por una impresora que ofrezca alta resolución de impresión garantizará textos claros e imágenes precisas. Asimismo, es recomendable verificar la velocidad de impresión, especialmente en hogares con

varios estudiantes o en entornos donde se necesiten grandes volúmenes de impresión en poco tiempo. Esto se evidencia en las impresoras de inyección de tinta con Tecnología Epson Heat-Free, pues al consumir menos energía, no solo ofrecen impresiones de alta calidad, sino que también reducen significativamente el costo por página, y ahorran hasta un 90% en impresiones en blanco y negro en comparación con alternativas láser.

Versatilidad en tipos y tamaños de papel

No todas las impresiones son en hojas tradicionales. Muchas veces, los estudiantes requieren imprimir en distintos tipos de papel, como cartulina para trabajos manuales o papel fotográfico para proyectos creativos. Una impresora que permita utilizar diversos materiales y tamaños facilitará la realización de proyectos escolares sin limitaciones. Modelos con impresión sin bordes y configuraciones automáticas para distintos gramajes de papel pueden ofrecer resultados más profesionales y adaptados a cada necesidad.

Conectividad y facilidad de uso

En un mundo cada vez más digital, la posibilidad de imprimir directamente desde dispositivos móviles y computadoras sin necesidad de cables no solo es una ventaja, sino se vuelve necesario. Modelos con conexión Wifi

permiten enviar documentos desde cualquier habitación de la casa, ahorrando tiempo y optimizando la experiencia de impresión. También es importante considerar opciones con aplicaciones intuitivas que ayuden a gestionar la impresora de una manera sencilla, directa y eficiente. Por ejemplo, con la aplicación Smart Panel de Epson, se puede imprimir, escanear documentos, o hasta verificar los niveles de tinta de la impresora desde el smartphone.

“El regreso a clases es una oportunidad clave para organizar el espacio de estudio en casa. Contar con una impresora que ofrezca calidad, eficiencia y facilidad de uso, como es el caso de la Epson L4260, es esencial para acompañar el proceso de aprendizaje. Este modelo, que forma parte de la línea EcoTank, destaca por su sistema de tinta de ultra alto rendimiento, conectividad con Smart Panel y bajo costo de impresión por página, lo que permite a los estudiantes imprimir más y preocuparse menos. Tiene impresión en ambas caras y un dúplex automático que permite ahorrar 50% de tiempo y papel al momento de imprimir. Equipos como este, que se adaptan a las necesidades de los alumnos, ayudan a optimizar el tiempo y los recursos”, comentó Daniel Hoyos, Product Manager de EcoTank y Consumibles en Epson Latinoamérica.



Mitchell Zhang, presidente de Huawei Enterprise América Latina

Huawei reunió a líderes y socios estratégicos en evento Eco Connect Summit 2025 realizado en México

Bajo el lema "Grow Together, Win the Intelligent Era", Huawei celebró con éxito una nueva edición de su evento insignia: el Huawei Latin America Eco-Connect Summit 2025, que reunió a líderes de la industria, socios estratégicos y expertos tecnológicos de toda la región. Durante dos días, el 24 y 25 de abril, la Ciudad de México se convirtió en el epicentro de la innovación digital para América Latina.

El evento presentó soluciones de vanguardia en conectividad, inteligencia artificial y ciberseguridad, abriendo nuevas oportunidades de negocio para industrias de todos los tamaños.

"Nuestra estrategia en América Latina se basa en fortalecer el desarrollo de mercados verticales y en la expansión conjunta con nuestros socios", destacó Mitchell Zhang, presidente de Huawei Enterprise América Latina. "Apostamos al crecimiento a través de la innovación tecnológica y sociedades sólidas que impulsen el desarrollo de las industrias clave de la región".

El evento combinó keynotes magistrales, paneles de expertos y demostraciones tecnológicas, donde Huawei expuso su visión de la "Era de la Inteligencia Total" (All Intelligence): un ecosistema donde la inteligencia artificial, los

datos y la conectividad 5G se integran para transformar la vida de las personas, optimizar procesos empresariales y fortalecer los servicios gubernamentales.

Huawei enfatizó además su modelo de colaboración total con socios estratégicos. Ricardo Matsui, vicepresidente de Desarrollo de Socios Empresariales para América Latina, subrayó: "La escucha activa y la mejora continua son fundamentales. El crecimiento de Huawei y de nuestros socios es recíproco; juntos mejoramos la experiencia del cliente y consolidamos nuestro impacto en el mercado".

Tecnologías disruptivas

Entre las innovaciones destacadas durante el Eco-Connect Summit estuvieron las soluciones de Wi-Fi 7, virtualización de centros de datos (DCS), redes de comunicación avanzadas (DCN) y nuevas plataformas de ciberseguridad. Estas tecnologías no solo optimizan los procesos actuales, sino que preparan a las empresas para un entorno digital en permanente evolución.

Huawei Eco-Connect Summit 2025 reafirma el compromiso de la compañía de construir una América Latina más conectada, más inteligente y resiliente, impulsando el crecimiento conjunto como camino para conquistar el futuro.

Samsung sigue liderando el mercado, seguido por Apple y Xiaomi



Canalys: el mercado mundial de smartphones

creció un modesto 0.2% en el primer trimestre de 2025

Según la última investigación de Canalys, en el primer trimestre de 2025, el mercado mundial de teléfonos inteligentes registró un ligero crecimiento del 0,2%, con envíos que alcanzaron los 296,9 millones de unidades. A medida que el ciclo pico de reemplazo llegó a su fin y los proveedores priorizaron niveles de inventario más saludables, el crecimiento del mercado mundial de teléfonos inteligentes se desaceleró por tercer trimestre consecutivo.

Samsung mantuvo su liderazgo, vendiendo 60,5 millones de unidades, respaldado por el lanzamiento de sus últimos modelos insignia y nuevos productos de la serie A a precios competitivos. Apple ocu-

pó el segundo lugar con 55.0 millones de unidades vendidas y una participación de mercado del 19%, impulsada por el crecimiento en los mercados emergentes de Asia Pacífico y Estados Unidos. Xiaomi obtuvo el tercer lugar con 41,8 millones de unidades enviadas y una cuota de mercado del 14%, aprovechando su diverso ecosistema de productos para fortalecer su marca en China continental y en los mercados emergentes de ultramar. Vivo y OPPO le siguieron en cuarto y quinto lugar, con envíos de 22,9 millones y 22,7 millones de unidades, respectivamente.

"El panorama regional de los teléfonos inteligentes se está volvien-

do cada vez más complejo", dijo Toby Zhu, analista principal de Canalys. "Los mercados que habían mostrado un fuerte impulso durante el año pasado, como India, América Latina y Oriente Medio, ahora están experimentando descensos notables en el primer trimestre de 2025, lo que indica una saturación en la demanda de reemplazo de productos del mercado masivo.

La mayoría de las marcas de Android ajustaron activamente los niveles de inventario en el primer trimestre para evitar interrupciones en los lanzamientos de nuevos productos y los precios de los canales. El mercado europeo también ha caído después de una breve re-

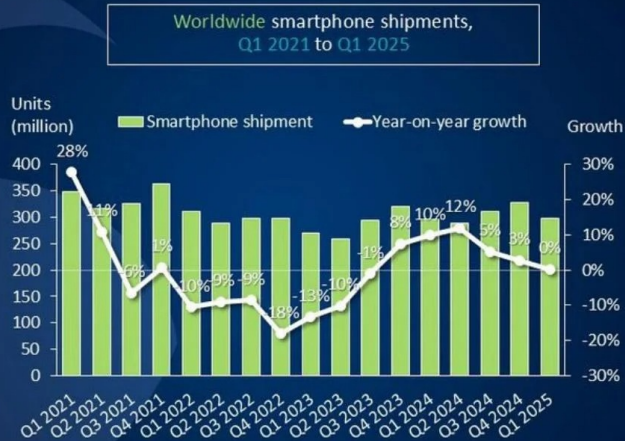
cuperación, con los proveedores enfrentándose a un alto inventario de productos insignia desde finales del año pasado e interrupciones en las líneas de productos de gama media y baja debido a la próxima directiva de diseño ecológico. No obstante, algunas regiones siguen mostrando una fuerte demanda. Los programas de subsidios del gobierno estimularon el crecimiento de China continental, mientras que África continuó beneficiándose de las vibrantes actividades minoristas y los esfuerzos proactivos de expansión del mercado.

Los proveedores aún pueden expandirse optimizando sus carteras de productos en este complejo entorno regional. Por ejemplo, Vivo y Honor lograron un crecimiento de dos dígitos en sus mercados extranjeros, con Honor alcanzando un máximo histórico en sus envíos al extranjero".

"El mercado de teléfonos inteligentes de EE.UU. se destacó, creciendo un 12% interanual en el primer trimestre, impulsado principalmente por Apple", dijo Le Xuan Chiew, gerente de investigación de Canalys. "Apple acumuló inventario de manera proactiva antes de las políticas arancelarias anticipadas. Si bien los iPhones producidos en China continental todavía representan la mayoría de los envíos de EE.UU., la producción en India aumentó hacia el final del trimestre, cubriendo los modelos estándar de las series iPhone 15 y 16, junto con la aceleración de la producción de la serie 16 Pro.

Con las continuas fluctuaciones en las políticas arancelarias recíprocas, es probable que Apple traslade aún más la producción con destino a EE.UU. a India para reducir la exposición a riesgos futuros. También se espera que los aranceles afecten de manera desproporcionada a los dispositivos de nivel de entrada, lo que podría reducir la disponibilidad de modelos de menor costo e impulsar los precios de venta promedio (ASP) más altos en los EE.UU.

The global smartphone market experienced a slowdown in growth for three consecutive quarters



Source: Canalys estimates (sell-in), Smartphone Analysis, April 2025

Omdia canalys

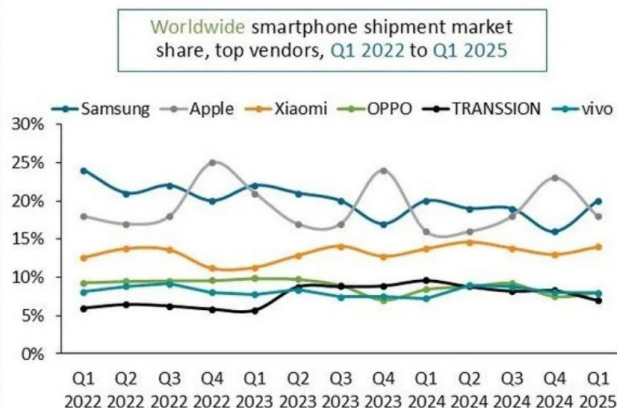
Estas dinámicas introducen nuevas incertidumbres no solo para Apple, sino también para las marcas de Android que compiten en el mercado. Las estrategias de fijación de precios, los paquetes de paquetes de los operadores y las futuras estructuras de productos se verán sometidos a una presión significativa. Mientras tanto, se espera que el mercado de teléfonos inteligentes de EE.UU. experimente una volatilidad considerable durante los próximos dos o tres trimestres, afectado por las correcciones de inventario y el debilitamiento de la confianza del consumidor".

"Las principales marcas de teléfonos inteligentes aún no han ajustado sus objetivos de envío para todo el año, a pesar del desempeño mediocre en el primer trimestre", declaró Zhu. "Siguen siendo optimistas sobre un repunte del mercado en el segundo trimestre y en la segunda mitad del año. Algunas regiones, como el sudeste asiático y América Latina, ya mostraron signos de recuperación gradual en

marzo. Además, la disminución de los niveles de inventario y el lanzamiento a mediados de año de nuevos productos de gama media y baja han aumentado su confianza. Sin embargo, los proveedores aún enfrentan múltiples desafíos.

En primer lugar, las marcas están adoptando un enfoque cauteloso para las actualizaciones de hardware en los segmentos del mercado masivo para compensar el aumento de los costos, lo que requiere una gestión más refinada de los ciclos de vida del producto, los precios y las estrategias de comercialización. En segundo lugar, la competencia en el segmento de gama media (entre 200 y 400 dólares) se intensificará a medida que las marcas busquen avances en los ASP. En tercer lugar, la posibilidad de una escalada de las tensiones comerciales mundiales podría llevar a más países a buscar la fabricación localizada de teléfonos inteligentes, lo que plantea presiones adicionales de inversión y costos para los proveedores".

Samsung took the lead in the global smartphone market in Q1 2025 as vendors focused on keeping their businesses healthy



**ESET Latinoamérica advierte
objetivos valiosos para**

¿Cuáles son los principales modelos de inteligencia



Fabiana Ramírez Cuenca, Investigadora
de seguridad informática de ESET
Latinoamérica.

Los modelos de inteligencia artificial se convirtieron en activos valiosos para ciber-criminales y en un objetivo atractivo para los ciberdelincuentes por la cantidad de información que procesan y por su uso cada vez

más frecuente en diversas industrias. En este contexto, ESET alerta que los ataques a los modelos de IA varían desde el robo de propiedad intelectual, filtrado de información -e incluso su manipulación para generar resultados erróneos, sesgados-, hasta la utilización de su infraestructura para propósitos maliciosos como, por ejemplo, el uso de servidores comprometidos para comandar redes de bots o ataques similares.

Existen una gran variedad de ejemplos de vulneraciones a modelos de IA. Algunos muy destacados como el de Tay de Microsoft, donde en el año 2016 un chatbot de IA fue manipulado por usuarios para aprender y replicar discursos de odio en menos de 24 horas. Por otro lado, el ataque a GPT-3/OpenAI, donde se identificaron intentos de extracción de información confidencial de modelos de OpenAI, consultas o peticiones específicas que inducían a revelar datos sensibles utilizados en su entrenamiento. Además, en 2023, el modelo desarrollado por Meta LLaMA fue filtrado antes de su lanzamiento y fue utilizado y accedido por terceros, lo que generó preocupación sobre la protección de modelos propietarios en entornos abiertos.

“Los ataques dirigidos ya han puesto foco en modelos de IA, su funcionamiento e infraestructura. La seguridad debe abordarse desde una perspectiva integral, protegiendo todas las capas del funcio-

e que los modelos de IA son
ra los cibercriminales

Principales ataques a inteligencia artificial?

namiento de esta tecnología, partiendo de datos de entrenamiento, implementación del modelo y luego posteriores fases de acceso o interacción con este”, comenta Fabiana Ramírez Cuenca, Investigadora de seguridad informática de ESET Latinoamérica.

Para comprender cómo podría la IA ser objetivo de ataque, el equipo de investigación de ESET desgana algunos de sus elementos básicos expuestos y sus vulnerabilidades. Entro lo destacado, se encuentran los datos, todos los modelos son alimentados con datos de entrenamiento que deben tener calidad y confiabilidad para garantizar el funcionamiento correcto de la tecnología. Estos datos podrían ser vulnerables y un cibercriminal podría introducir algunos de tipo malicioso y de esa manera manipular el comportamiento o los outputs del modelo.

Por otro lado, están las APIS (Application Programming Interface) que al estar expuestas también se pueden intervenir para manipular el modelo o extraer información sensible, y la estructura interna del modelo, inclusive sus algoritmos, podrían ser susceptibles a ataques adversariales o extracción de información confidencial. Finalmente, los servidores, fuera de ataques al funcionamiento del modelo en sí, este se podría ver afectado en caso de que los servidores o bases de datos donde se almacene su información o se procese

el modelo sean blanco de diversos ataques que interrumpen el sistema.

Estos son los principales ataques a modelos de IA

Data Poisoning (Envenenamiento de datos)

Consiste en la manipulación de los datos de entrenamiento con el objetivo de alterar el comportamiento del modelo.

Ataques adversariales

Se generan inputs o entradas manipuladas de manera casi imperceptible para los humanos, pero que inducirán errores en el modelo. Por ejemplo, la manipulación de imágenes para hacer que un modelo de reconocimiento facial confunda identidades.

Control del modelo y explotación

Los cibercriminales toman el control del modelo durante su producción aprovechándolo con distintos fines como ejecución de otros ataques. Por ejemplo, una denegación de servicio aprovechando para generar comando y control (C&C) e incluso mezclarlo con bots.

Model Inversion Attack (Inversión de modelo)

El objetivo es inferir y obtener información sensible a partir de las predicciones del modelo. Por ejemplo, en modelos que identifican datos faciales se podría llegar reconstruir

los rostros originales tomando como base los resultados del modelo frente a ciertas peticiones.

Model Extraction Attack (Extracción de modelo)

En este tipo de ataque se envían diferentes consultas al modelo para luego analizar las salidas con el objeto de entender y reconstruir su estructura interna, así como su lógica. De esta manera se podría imitar o replicar un modelo sin necesidad de acceso directo al código fuente o datos de entrenamiento.

Ataque de evasión (Evasion Attack)

Para el caso se modifican los inputs de los modelos con el fin de evadir detección de ciertas actividades o generar una clasificación errónea. Se ha utilizado en sistemas de detección de fraudes, por ejemplo, y en modelos de seguridad de tipo antimalware y firewalls basados en IA. Los atacantes utilizan códigos maliciosos que puedan generar que el modelo víctima clasifique un archivo como legítimo, por ejemplo, y esto mediante generación de inputs alterados de forma imperceptible.

Malware en infraestructuras

Fuera de ataques directos al modelo, estos están sujetos a que sus servidores sean infectados con diferentes clases de malware que pudiera interrumpir su operatividad, bloquearlos e incluso lograr filtrar información.



La inteligencia artificial d
convertirse en una he

IA colabora desarrolladores las claves de Google ya impactan a A

En Las Vegas, Google Cloud Next 2025 reunió a más de 700 ponencias y miles de asistentes de todo el mundo para mostrar cómo la inteligencia artificial (IA) ya no es una visión futurista, sino una tecnología que está revolucionando la forma en que trabajamos, creamos y tomamos decisiones.

Y no se trata solo de Silicon Valley. Empresas latinoamericanas, como Orión, socio estratégico de Google Cloud con presencia regional, participaron activamente del evento, compartiendo aprendizajes y tendencias que ya están tocando nuestra región. “La IA ya no es una herramienta para unos pocos. Hoy es una capacidad estratégica para quienes quieren liderar su industria”, comentó Carlos Honorato, CEO de Orión, en conversación tras su paso por el evento.

¿Qué viene para las empresas y profesionales en Perú?

Orión presenta cinco claves que marcarán el rumbo de la innovación tecnológica en los próximos años:

1. Modelos de IA más veloces y creativos

Gemini 1.5 Flash, Imagen 3 y Lyria son algunas de las nuevas apuestas de Google para crear texto, imágenes, música e incluso voces sintéticas a partir de unos segundos de muestra. Estos modelos estarán disponibles a través de herramientas como Vertex AI y AI Studio, abriendo la puerta a nuevas formas de automatización y creativi-

dad, incluso para pequeñas y medianas empresas.

2. Agentes inteligentes: tu próximo colega será una IA

Google presentó kits de desarrollo para construir agentes virtuales capaces de razonar, tomar decisiones y ejecutar tareas complejas. Herramientas como el Agent Development Kit (ADK) permitirán crear asistentes que trabajen a la par de humanos, agilizando flujos en áreas como finanzas, logística, ventas y atención al cliente.

3. Infraestructura de alto rendimiento para IA

Con la arquitectura AI Hypercomputer, Google ofrece un ecosistema capaz de entrenar modelos avanzados con menos consumo energético y mayor velocidad. Esto incluye nuevas TPU y GPU de última generación, así como



dejó de ser promesa para
herramienta transversal

Colaborativa y empoderados Cloud Next 2025 que América Latina

máquinas virtuales optimizadas. Para las empresas peruanas que ya están explorando soluciones de IA, esto significa más poder de cómputo con menos costos.

4. Desarrollo y almacenamiento sin límites

El desarrollo colaborativo y el manejo de datos a gran escala serán cada vez más ágiles. Soluciones como Hyperdisk Exapools y Rapid Object Storage buscan reducir la latencia a menos de un milisegundo, algo clave en sectores como banca, minería o e-commerce local, donde los datos en tiempo real son oro.

5. Seguridad y cumplimiento desde la nube

Google también puso foco en la ciberseguridad y la interoperabilidad. Con Google Unified Security (GUS) y el uso de Gemini en entornos de nube distribuida, se garantiza la protección de datos sensibles, algo clave para industrias reguladas como la salud o la educación. Además, la adopción de estándares abiertos facilitará el trabajo entre plataformas y empresas.

¿Y Perú?

Aunque aún existen desafíos como la brecha digital, la falta de talento especializado y la necesidad de mayor inversión en I+D, las oportunidades están sobre la mesa. La inteligencia artificial ya no es algo que vendrá: está aquí, y las empresas peruanas que sepan integrarla estratégicamente tienen todo para liderar en sus sectores.

Como dijo Honorato: “Desde cómo se diseña una película hasta cómo se optimiza un proceso financiero, la IA ya es parte del ADN empresarial. El futuro del trabajo será colaborativo, no solo entre humanos, sino también entre humanos e inteligencias artificiales”.





Con procesador AMD HP presenta en Perú a la n



HP ha lanzado en el mercado peruano la nueva HP OmniBook Ultra 14, una laptop de última generación impulsada por el procesador AMD Ryzen AI Serie 300, diseñada para quienes buscan rendimiento, portabilidad, seguridad y una experiencia personalizada gracias a la inteligencia artificial. Este modelo fue presentado oficialmente ante prensa especializada, so-

cios estratégicos y entusiastas de la tecnología el pasado 24 de abril.

"La OmniBook Ultra 14 representa el futuro del cómputo personal. No solo es una herramienta de trabajo y entretenimiento, sino un verdadero asistente inteligente que aprende y se adapta a cada usuario. Responde a una visión más amplia desde HP, que es liderar lo que llamamos el Future of Work, con dispositivos diseñados para transitar de forma fluida entre el trabajo y el entretenimiento", afirmó Cecilia Bejarano, gerente de Ventas de Canales de HP Perú y Bolivia.

Este equipo es una integración total de soluciones de hardware, software y servicios, que permite a los usuarios vivir una experiencia unificada, fluida y confiable. Incorpora herramientas avanzadas para editar fotos y videos al instante, gracias a sus

gráficos Radeon 800M y un procesador de última generación con una Unidad de Procesamiento Neuronal dedicada (NPU) de 55 TOPS. Además, cuenta con una batería que dura hasta 22 horas y un diseño ultraligero hecho con materiales reciclados, perfecto para acompañarte durante todo el día.

Desde AMD, Giovanni Orezza, Consumer Sales Manager para Perú y Ecuador, comentó: "La vida digital actual exige dispositivos versátiles, capaces de adaptarse sin esfuerzo a distintos escenarios de productividad, creatividad y entretenimiento. En ese sentido, la nueva HP OmniBook Ultra, equipada con los procesadores AMD Ryzen AI 9 HX 375, representa un avance significativo. Estos procesadores cuentan con una arquitectura "Zen 5" de alto rendimiento, con hasta 12 núcleos y 24 hilos, lo que



D Ryzen AI Serie 300

nueva OmniBook Ultra 14

permite alcanzar un rendimiento ultrarrápido en laptops ultradelgadas y premium. Además, gracias a la nueva arquitectura AMD XDNA 2, ofrecen un motor de inteligencia artificial que optimiza tareas locales, acelera la generación de contenido y automatiza flujos de trabajo, todo con una eficiencia energética excepcional”.

Incorpora la mejor tecnología de HP

Esta laptop también incorpora el HP AI Companion como un nuevo asistente virtual personal. Este sistema ayuda a organizar archivos, resolver dudas, sugerir nuevas herramientas e incluso mantener el equipo actualizado, todo mientras aprende del comportamiento del usuario para personalizar la experiencia.

En cuanto a seguridad, este equipo integra HP Wolf Security, una solu-

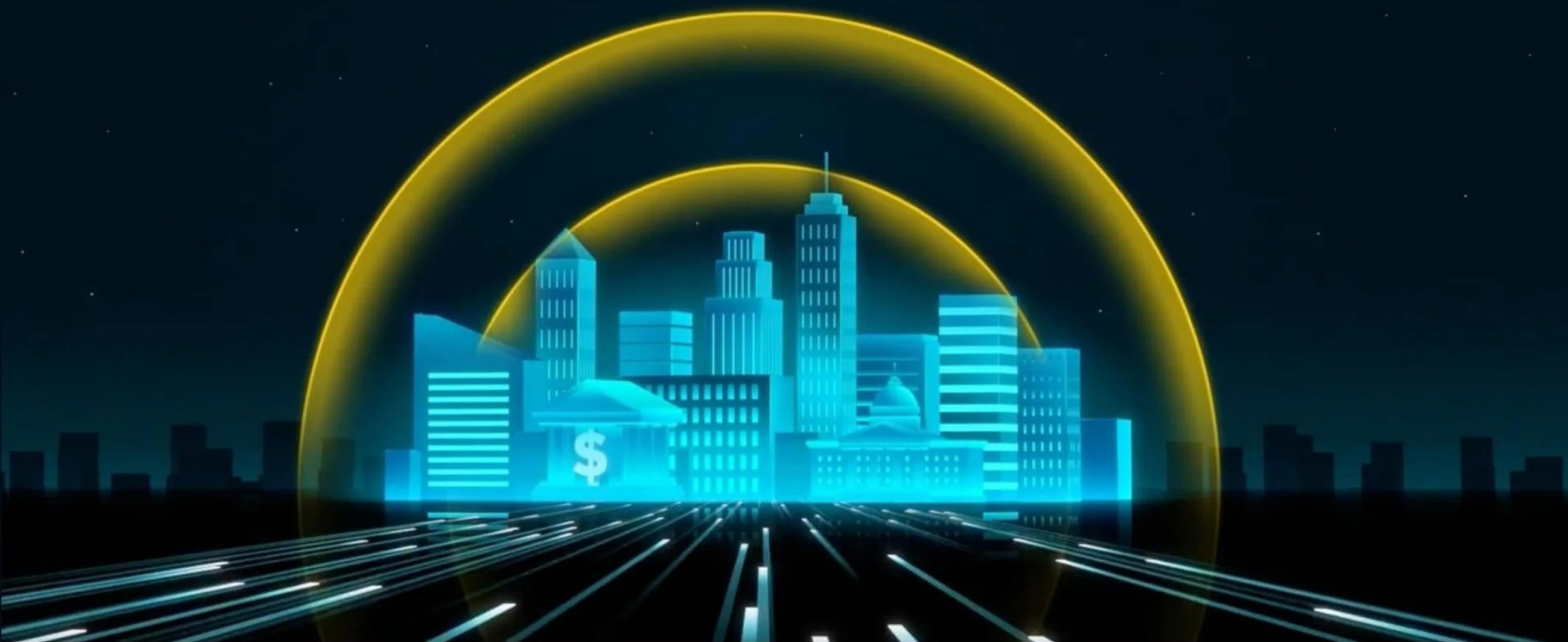
ción avanzada con un chip único que permite al núcleo del dispositivo auto repararse frente a ciberataques o cualquier amenaza maliciosa al equipo, protegiendo datos personales y preservando la privacidad del usuario.

La experiencia audiovisual también ha sido llevada a otro nivel. Gracias a la cámara de 9MP con tecnología Poly Camera Pro y a las funciones de Microsoft Studio Effects y Poly Studio, las videollamadas ofrecen una calidad de imagen y sonido excepcionales, permitiendo una comunicación más auténtica y profesional desde cualquier lugar.

Por otro lado, este es un equipo que también lleva consigo el compromiso de HP con el cuidado del planeta: ha sido fabricada con materiales reciclados posconsumo y cuenta con la cer-

tificación EPEAT Gold con Climate+. Disponible próximamente en los principales puntos de venta del país, la nueva HP OmniBook Ultra 14 está pensada para usuarios exigentes que buscan rendimiento, diseño, inteligencia y responsabilidad ambiental, todo en un solo equipo.

Desde laptops como la recién presentada, hasta soluciones en seguridad, colaboración y sostenibilidad, HP ofrece un ecosistema completo de dispositivos y herramientas potenciadas por inteligencia artificial que están redefiniendo la manera de trabajar y crear. Con ello, la marca consolida su posición como el proveedor con el portafolio más amplio de soluciones tecnológicas con IA, ofreciendo experiencias personalizadas, eficientes y potentes, tanto para usuarios individuales como para organizaciones.



Palo Alto Networks anuncia Prisma AIRS, una plataforma de seguridad con IA que sirve como base para una protección robusta contra la IA generada por la ciberdelincuencia.

Prisma AIRS está diseñada para proteger todo el ecosistema de IA empresarial (aplicaciones, agentes, modelos y datos de IA) en cada paso. Basándose en la cartera de productos Secure AI by Design de la compañía, lanzada el año pasado, Prisma AIRS permite a los clientes implementar la IA con valentía y abordar la necesidad crítica de una seguridad robusta ante la rápida adopción de la IA en las empresas.

Las empresas están adoptando rápidamente esta tecnología, implementando aplicaciones de IA y LLM en prácticamente todas las funciones, desde la atención al cliente hasta la generación de códigos, impulsando la innovación, pero también introduciendo puntos ciegos, riesgos y vulnerabilidades de seguridad. Para proteger de forma más eficaz las iniciativas de IA y prevenir incidentes de seguridad, las organizaciones necesitan una plataforma integral de seguridad de IA como Prisma AIRS, la cual utiliza la mejor seguridad para proteger todo el ecosistema de IA, permitiendo a las organizaciones implementarla con la confianza de que todo lo que crean es seguro.

“A medida que las organizaciones integran la IA en todos los aspectos de sus operaciones, su seguridad requiere

una plataforma de seguridad en tiempo de ejecución que proporcione visibilidad continua e información en tiempo real. Sin esto, los equipos de seguridad desconocen cómo se utiliza, se utiliza indebidamente o se manipula la IA, lo que pone en riesgo datos y decisiones críticas. Prisma AIRS proporciona a los equipos respuestas a preguntas esenciales, como si alguien está explotando un LLM para extraer información confidencial o si una API comprometida está alimentando el modelo con datos contaminados. Esta información es vital para mantener la confianza y proteger la IA”, aseguró Anand Oswal, vicepresidente sénior y director general de Palo Alto Networks:

Una solución con múltiples capacidades

Prisma AIRS incluye múltiples capacidades como el escaneo de modelos de IA, una herramienta que permite la adopción segura de modelos de IA analizándolos en busca de vulnerabilidades. Esto protege el ecosistema de IA contra riesgos como la manipulación de modelos, scripts maliciosos y ataques de deserialización.

Asimismo, también cuenta con Gestión de la postura, que recaba información sobre los riesgos de la postura de seguridad asociados con el ecosistema de IA, como permisos excesivos, exposición de datos confidenciales, configuraciones incorrectas de la plataforma, configuraciones incorrectas de acceso y más.

Otra gran innovación es el Red Teaming de IA. Esta valio-

Para proteger el ecosistema de IA: aplicaciones, agentes, modelos y datos

Palo Alto Networks lanza la plataforma de ciberseguridad Prisma AIRS

sa herramienta descubre posibles exposiciones y riesgos latentes antes de que lo hagan los atacantes y realiza pruebas de penetración automatizadas en sus aplicaciones y modelos de IA con el agente de Red Teaming de Palo Alto Networks, el cual somete a pruebas de estrés las implementaciones de IA, aprendiendo y adaptándose como un atacante real.

Por otro lado, la Seguridad en tiempo de ejecución protege las aplicaciones, modelos y datos de IA impulsados por LLM, mientras que la Seguridad de agentes de IA protege a los agentes, incluidos aquellos creados en plataformas sin código o con poco código, contra nuevas amenazas agénticas. Estos dos enfoques ayudan a repeler amenazas en tiempo de ejecución, como inyección de indicaciones, código malicioso, contenido tóxico, fuga de datos confidenciales, sobrecarga de recursos, así como suplantación de identidad, manipulación de memo-

ria y uso indebido de herramientas.

“Los agentes y las aplicaciones de IA están transformando nuestra forma de trabajar y vivir. Al mismo tiempo, la superficie de ataque no solo se está expandiendo, sino que está cambiando radicalmente. Lo último que necesitan las organizaciones son más productos específicos para proteger su uso de la IA. Las organizaciones necesitan la mejor seguridad de su clase, proporcionada mediante la arquitectura adecuada; la platformización es esa arquitectura. Prisma AIRS aborda tanto las amenazas tradicionales como las específicas

de la IA con capacidades de seguridad de primera clase, entregadas en una plataforma de seguridad de IA integral y unificada que permite a las organizaciones implementar la IA con valentía”, sentenció Lee Klarich, director de producto de Palo Alto Networks.



Ejecuta acciones con lenguaje natural gracias a plugins personalizados.

NVIDIA presenta Project G-Assist

Asistente inteligente para ajustar y controlar PC con tarjetas GeForce RTX

La inteligencia artificial está transformando rápidamente lo que se puede hacer con una computadora. Desde la generación de imágenes en tiempo real hasta flujos de trabajo controlados por voz, las posibilidades se expanden cada día. Pero mientras las capacidades de la IA crecen, también lo hace su complejidad. Aprovechar todo su potencial muchas veces significa trabajar en configuraciones técnicas, ajustes de sistema y compatibilidad de hardware y software.

Pensando en esto, NVIDIA presenta Project G-Assist, un asistente inteligente diseñado para optimizar, ajustar y controlar PC con tarjetas GeForce RTX. Esta función ya está disponible en la app de NVIDIA, y permite a los usuarios interactuar mediante comandos de voz o texto para tareas como monitorear el rendimiento, cambiar configuraciones e incluso comunicarse con periféricos compatibles. Incluso se pueden invocar otras IAs potenciadas por RTX directamente desde la computadora.

Pero eso no es todo. Para aprovechar más G-Assist, ahora se pueden crear complementos con el nuevo G-Assist Plug-In Builder, una herramienta basada en ChatGPT que permite a desarrolladores y entusiastas personalizar su funcionalidad. Se pueden añadir nue-

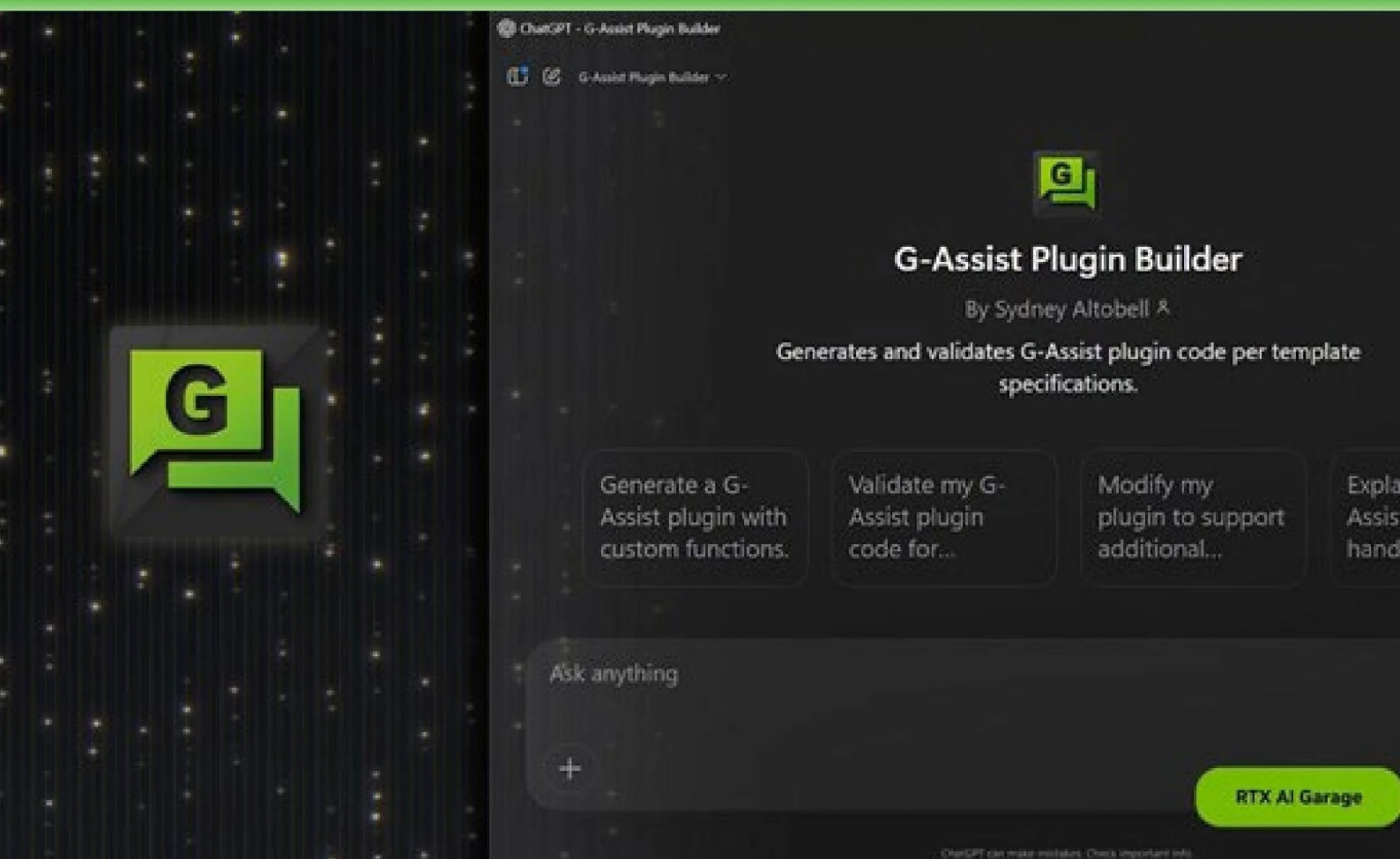
vos comandos, conectar herramientas externas o diseñar flujos de trabajo de IA adaptados a necesidades específicas. Esta herramienta genera automáticamente el código necesario (en el formato correcto) y lo integra a G-Assist para que la PC responda rápidamente a comandos de voz o texto.

¿Qué son los plug-ins y cómo funcionan?

Los plug-ins son pequeños complementos que le añaden nuevas funciones a un programa. En el caso de G-Assist, estos pueden controlar música, conectarse con modelos de lenguaje grandes y mucho más. Internamente, los plug-ins usan APIs (interfaces de programación) para comunicar diferentes programas entre sí. Se pueden definir funciones usando archivos JSON sencillos, escribir la lógica en Python, e integrarlos de manera rápida y efectiva.

Con el Plug-In Builder, los usuarios pueden:

- Usar un modelo de lenguaje pequeño que corre localmente en la GPU RTX, para respuestas rápidas y privadas.
- Expandir las capacidades de G-Assist con funciones personalizadas para flujos de trabajo, videojuegos o herramientas favoritas.



- Interactuar con G-Assist desde la superposición de NVIDIA, sin tener que salir de lo que se está haciendo.
- Controlar el GPU y otras funciones del sistema desde aplicaciones usando C++ o Python.
- Integrarlo en flujos de trabajo complejos usando herramientas como Langflow, conectando G-Assist con otros agentes inteligentes.

Construido para creadores: API gratuitas para mejorar la experiencia

NVIDIA ofrece todo lo necesario en su repositorio de GitHub para comenzar a desarrollar: ejemplos de plugins, guías paso a paso y documentación completa. Solo se tienen que crear funciones en JSON, colocar los archivos de configuración en la carpeta correspondiente y G-Assist los detectará automáticamente. Además, los usuarios pueden enviar plug-ins para que se revisen y, si son aprobados, se publiquen en el GitHub de NVIDIA para que sean utilizados por otros usuarios.

Además, existen cientos de API gratuitas que se

pueden aprovechar —ya sea para automatizar tareas, mejorar el rendimiento de la PC o hasta para hacer más eficiente la experiencia de compras en línea. Se pueden encontrar opciones en sitios como publicapis.dev, free-apis.github.io, apilist.fun y API-Layer.

Entre los plug-ins destacados ya disponibles se encuentra Spotify que controla música y volumen sin manos. Google Gemini usa una IA más robusta en la nube para conversaciones más complejas, ideas o búsquedas web usando Google AI Studio API.

Twitch Plug-In: un desarrollador que crea un complemento que le permite a G-Assist decir si un streamer está en vivo con solo preguntarle por voz. Da clic en este enlace para ver más detalles.

También se pueden controlar periféricos compatibles y apps con comandos como ajustar ventiladores, hacer benchmarks o cambiar la iluminación de dispositivos de Logitech G, Corsair, MSI y Nanoleaf. En este video se pueden ver más detalles al respecto.

Otros plugins útiles son Stock Checker que consulta precios de acciones en tiempo real y Weather Plug-In que da el clima actual en cualquier ciudad del mundo.

SUSCRÍBETE al Boletín Canal TI

Somos una revista de frecuencia semanal en América del Sur.
Haz que Canal TI llegue a todos los integrantes de tu empresa, amigos y contactos del negocio TI



Aquí encontrarás todas las noticias e información del negocio TI que necesitas para tomar las mejores decisiones de negocio

- AVANCES TECNOLÓGICOS
- NOMBRAMIENTOS
- PREMIACIONES
- PROMOCIONES Y OFERTAS
- RECIENTES LANZAMIENTOS

Todos los lunes



RECIBE NUESTRO BOLETIN
DIGITAL

Inscríbe tu correo

Visita www.canalti.pe